

GS224-2

أمن المعلومات



أهمية

أمن المعلومات



الاهداف :-

- التعريف بأمن المعلومات.
- توضيح الحاجة إلى أمن المعلومات، وأنها ضرورة ملحة، وليست حلولاً اختيارية.
- التعرف إلى تهديدات أنظمة أمن المعلومات، كأحد الأسباب الرئيسة للحاجة إلى أمن المعلومات.
- التعرف إلى الهجمات الإلكترونية وخطورتها على المعلومات والأنظمة المعالجة لها، مع إبراز الحاجة إلى أمن المعلومات لمجابهتها.

1- أمن المعلومات

إنَّ علم أمن المعلومات هو العلم الذي يُعنى بحماية المعلومات من المخاطر التي قد تتعرَّض لها. ويمكن تعريف أمن المعلومات بشكل مختصر بأنه: «حماية المعلومات من الوصول غير المسموح به». ويمكن تعريفه بتفصيل أكثر بأنه: «المفاهيم والتقنيات والتدابير التقنية والإدارية المستخدمة لحماية أصول المعلومات من الوصول غير المأذون به عمدًا أو سهوًا أو حيازتها أو الإضرار بها، أو كشفها، أو التلاعب بها، أو تعديلها، أو فقدانها أو إساءة استخدامها»^١. تعرّف لجنة أنظمة الأمن القومي الأمريكية (Committee on National Security Systems- CNSS)^٢ أمن المعلومات بأنه: «حماية المعلومات وعناصرها المهمة (الدرجة) بما في ذلك الأنظمة والأجهزة التي تُستخدم هذه المعلومات وتخزينها وترسلها»^٣.

► 3

2- محاور مفهوم أمن المعلومات

- حماية المعلومات من الضرر بأشكاله كافة، سواءً أكان مصدره أشخاص (كالمخترقين)، أم برامج (كفيروسات الحاسب الآلي)، وسواءً أكان متعمدًا أم عن طريق الخطأ.
- حماية المعلومات من الوصول غير المصرح به، أو السرقة، أو الالتقاط، أو التغيير، أو إعادة التوجيه، أو سوء الاستخدام.
- حماية قدرة المنشأة على الاستمرار وأداء أعمالها على أحسن وجه.
- تمكين أنظمة تقنية المعلومات والبرامج التطبيقية لدى المنشأة من العمل بشكل آمن.

►



3- موجبات أمن المعلومات

1

حماية الأصول المعلوماتية الحرجة: إذ لا تقوم تقنية المعلومات في المنشأة، ولا الخدمات التي تقدمها تلك المنشأة، إلا على أصول معلوماتية مهمة ودرجة يجب حمايتها من أي أخطار تهددها، ويجب المحافظة على استمراريتها وبقيائها متاحة متوافرة في جميع الأوقات. فالحاجة لحماية هذه الأصول تأتي من وجهين: الوجه الأول أنه لا يمكن للمنشأة أن تستمر دون بقاء هذه الأصول عاملة متاحة آمنة، والوجه الآخر أن توفير هذه الأصول كلف مبالغ وجهوداً كبيرة تستحق أن يُبذل من أجلها الوقت والجهد والمال لحمايتها، ومن الأمثلة على الأصول المعلوماتية الحرجة ما يلي:

- مراكز البيانات
- قواعد البيانات
- أجهزة الخوادم الرئيسية
- شبكات المحلية و المترامية
- أنظمة التشغيل
- البرامج التطبيقية
- أجهزة تخزين المعلومات
- المواقع الإلكترونية

3- موجبات أمن المعلومات

2

حاجة أعمال المنشآت وأنشطتها إلى ذلك: حيث أصبحت المعلومات تشكل ثروة حقيقية للمنشآت ومورداً مهماً من مواردها، بل إن المعلومات في بعض المنشآت هي مصدر الدخل الأول لها، ويقوم عليها نشاط المنشأة الأساسي، والتجارة الإلكترونية خير مثال لذلك.

3

حاجة المستفيدين من الخدمات الإلكترونية إلى ذلك: ومعنى ذلك أن المستفيدين من الخدمات الإلكترونية بحاجة إلى حماية معلوماتهم من كل ما يضر بها.

4

انتشار الخدمات الإلكترونية عن بعد: مثل خدمات الحكومات الإلكترونية والتعليم عن بُعد، لدرجة أن المواطن يستطيع أن يُنهي جلّ أو جميع إجراءاته، وأن يحصل على درجته العلمية المناسبة من منزله.



3- موجبات أمن المعلومات

5 الحاجة إلى معرفة إمكانيات المنشآت ومدى قدرتها على حماية معلوماتها ومعرفة التهديدات التي تواجهها: فلكي تكون آمناً، فلا بد أن تعرف نفسك، وتعرف التهديدات التي تواجهك.

6 كثرة التهديدات المعلوماتية وتنوعها، وتعدد مصادرها: والخطورة في ذلك أنه قد توجد جملة من التهديدات داخل المنشأة، في أنظمتها المعلوماتية أو في موظفيها، إذا لم يُحاط لها فقد تضر بالمعلومات.

7 انتشار الهجمات الإلكترونية: ما انفكت وسائل الإعلام - على اختلاف أنواعها - تطالعنا من حين إلى آخر بالمزيد من أخبار الهجمات الإلكترونية، واختراق الشبكات، وتدمير الأنظمة، وظهور فيروسات الحاسب الآلي.

4- تهديدات المعلومات و انظمتها

التهديدات المحيطة بالمعلومات والأنظمة والتجهيزات التي تتعامل معها، إما بتخزين أو معالجة أو نقل. فهناك تهديدات كثيرة تحيط بأنظمة المعلومات شأنها في ذلك شأن أي نظام مفتوح يمكن الوصول إليه بعدة طرق، ومن قبل أشخاص مختلفين وفي أوقات مختلفة.

- 1. التهديدات الفنية :** الناجمة عن القصور و الأخطاء الفنية في مختلف أنظمة المعلومات والتي يغلب عليها الطابع الفني او تكون بسبب كارثة طبيعية
 - تهديدات عيوب التصنيع و التشغيل : عيوب التصميم في الاجهزة و البرامج و الشبكات و ادوات الربط و التخزين او أى مكون اخر من مكونات أنظمة المعلومات .
 - تهديد تشتت المعلومات : تشتت معلومات المنشأة على أماكن متعددة و يجرى التعامل معها من خلال شبكات متعددة مما يحتم تطبيق أنظمة معلومات متعددة - حسب الأماكن- مما يتسبب في ضعف منظومة الامن و زيادة تكلفتها



4- تهديدات المعلومات و انظمتها

2. **التهديدات البشرية :** الناجمة عن العنصر البشرى مباشرة , فقد يتسبب العنصر البشرى – عمدا او خطأ – فى الضرر او الوصول الى المعلومات و الاطلاع عليها دون ان يكون له صلاحية فى ذلك أو اتلافها او اطلاعها لجهات خارجية.
- المستخدم الشرعى الفاسد
 - موظف المرفق الفاسد
 - المستخدم و الموظف الغير واعيين للمخاطر الامنية
 - المؤسسات التجارية المنحرفة
 - المنظمات الارهابية
 - موردو الاجهزة و البرمجيات
 - المهندسون و المبرمجون و فنيو الصيانة و الدعم الفنى الخارجيون
3. **التهديدات الطبيعية :** ويقصد بها الكوارث الطبيعية التى ليس للانسان و التجهيزات الفنية دخل في حدوثها ، كالزلازل و البراكين و الفيضانات و الحرائق و غيرها .



5- التحديات التي تواجه نظم امن المعلومات

- (1) أمن المعلومات و الحاسبات ليس بالأمر السهل
- (2) يجب على المرء أن يفكر في الهجمات المحتملة (غير المتوقعة)
- (3) غالباً ما تكون الإجراءات المستخدمة غير بديهية
- (4) يجب أن يقرر مكان نشر آليات و نظم أمن المعلومات
- (5) تتضمن استخدام الخوارزميات ومعلومات سرية (مفاتيح سرية)
- (6) معركة ذكاء بين المهاجم / المشرّف
- (7) لا يُنظر إليه على أنها ذات منفعة حتى الفشل او الاختراق
- (8) تتطلب مراقبة و متابعة مستمرة
- (9) في كثير من الأحيان هي إجراءات وأفكار لاحقة (ليست متكاملة)
- (10) تعتبر عقبة أمام استخدام النظام

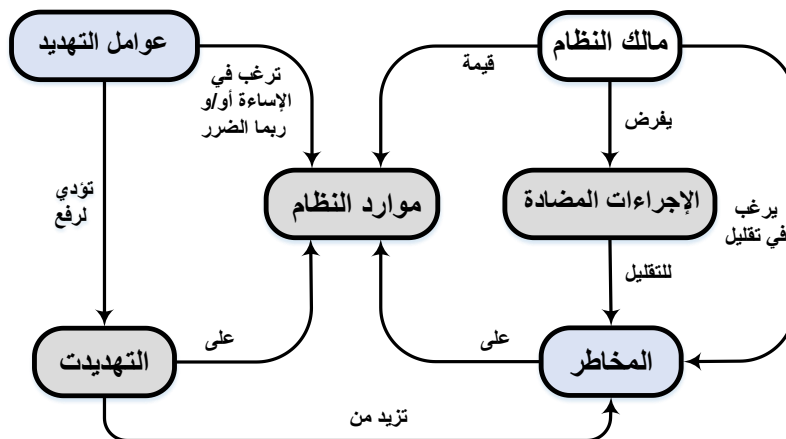


6- نموذج نظام أمن المعلومات

- موارد النظام
- الكيان المادي، البرمجيات (نظم التشغيل، التطبيقات)، البيانات (المستخدمين، النظام، قاعدة البيانات)، الشبكات و وسائل الاتصال (الموجهات، الجسور، الشبكة المحلية)
- قابلية الإصابة و ضعف موارد النظام : فساد ، عدم توفر الخدمة أو تسرب البيانات .
- التهديدات التي تستغل قابلية الإصابة أو الضعف
- الهجوم هو التنفيذ الفعلي لتهديد ما
- نشط أو سلبي ، من الداخل أو من الخارج
- الإجراءات المضادة : الاعمال المتخذة لمنع، كشف، استرداد و تقليل المخاطر



مفاهيم وعلاقات الأمن



7- مصطلحات أمن المعلومات

- ▶ **الخصم (عامل التهديد):** كيان مهاجم أو ما يمثل تهديدًا لنظام ما.
- ▶ **الهجوم :** اعتداء على أمن النظام نابع من تهديد ذكي ؛ وهو عمل ذكي في محاولة متعمدة (بمعنى كطريقة أو تقنية) للتهرب من الخدمات الأمنية وانتهاك السياسة الأمنية للنظام.
- ▶ **الإجراء المضاد:** إجراء أو تقنية تقلل من تهديد أو ثغرة أو هجوم أمني عن طريق التخلص منه أو منعه ، التقليل من الضرر الذي يمكن أن يسببه ، أو عن طريق اكتشافه والإبلاغ عنه بحيث يمكن اتخاذ إجراءات تصحيحية.
- ▶ **المخاطر:** توقع خسارة بحيث يتم التعبير عنها باحتمال أن يستغل تهديد معين ثغرة أمنية معينة مما ينتج عنه ضرر ما (عالي، متوسط، منخفض).
- ▶ **السياسة الأمنية :** مجموعة من القواعد والممارسات التي تحدد أو تنظم كيفية قيام نظام أو مؤسسة بتقديم خدمات الأمان لحماية موارد النظام الحساسة والحرية.
- ▶ **مورد النظام (الأصول) :** البيانات المخزنة بنظام المعلومات ؛ أو خدمة التي يقدمها النظام ؛ أو قدرات النظام مثل المعالجة أو عرض نطاق الاتصالات ؛ أو عنصر من معدات النظام (مثال ، أحد مكونات النظام -الأجهزة أو البرمجيات الثابتة أو اللوئاق) ؛ أو المنشأة تضم عمليات ومعدات النظام.
- ▶ **التهديدات :** احتمال انتهاك للأمن ، والذي يحدث عندما يكون هناك ظرف أو قدرة أو إجراء أو حدث يمكن أن ينتهك الأمن ويسبب ضررًا. أي أن التهديد هو خطر محتمل قد يستغل إحدى نقاط الضعف.
- ▶ **الوهن :** خلل أو ضعف في تصميم النظام أو تنفيذه أو تشغيله وإدارته يمكن استغلاله لانتهاك سياسة أمن النظام

▶ 13

8- عواقب التهديدات و الهجمات الناتجة

- **إفشاء غير مصرح به (Unauthorized disclosure) :** تهديد للسرية
 - **التعرض:** بيانات حساسة تم الإفصاح عنها مباشرة لجهة غير مرخص لها
 - **الاعتراض:** جهة غير مرخص لها تتواصل مباشرة مع بيانات حساسة أثناء الانتقال.
 - **الاستدلال:** يصل كيان غير مصرح به بشكل غير مباشر إلى بيانات حساسة من خلال الاستدلال على خصائص أو منتجات ثانوية للاتصالات.
 - **التطفل:** كيان غير مصرح به يقوم بالتحايل على تدابير الحماية الأمنية للنظام.
 - **الخداع (Deception):** تهديدًا لسلامة النظام أو نزاهة البيانات
 - **التنكر:** كيان غير مصرح له يتظاهر بأنه كيان مرخص له.
 - **التزوير:** بيانات كاذبة تخدع الجهة مرخص لها.
 - **التنصل:** كيان يخدع شخصًا آخر بإنكار المسؤولية عن فعل ما.
 - **الاخلال (Disruption) :** تهديدًا للتوافر أو النزاهة
 - **العجز:** منع / مقاطعة تشغيل النظام عن طريق تعطيل أحد مكونات النظام
 - **الفساد:** التعديل السلبي لوظائف أو بيانات النظام
 - **العوائق:** مقاطعة تقديم خدمات النظام عن طريق إعاقة تشغيل النظام.
 - **الاغتصاب (Usurpation) :** تهديد لسلامة النظام
 - **الاختلاس:** التحكم المنطقي أو المادي غير المصرح به لمورد النظام (سرقة الخدمة).
- سوء الاستخدام: يتسبب في قيام النظام بأداء وظيفة أو خدمة تضر بالأمن.



9- الهجمات الالكترونية و الحماية منها

تشكّل المعلومات في عصرنا الحاضر رافداً مهماً في حياة الدول والشعوب. وكثيرها من الروافد المهمة، فإنّه يحيط بها عدد من المخاطر أو الأعداء يجب حمايتها منهم، وكلّ خطر أو عدوّ من هؤلاء الأعداء لديه طرقه وأساليبه التي يستخدمها للوصول إلى هذه المعلومات، وبمجرّد النفاذ إلى المعلومات، فإنّه يمكن له نسخ أو تعديل أو حذف أو إساءة استخدامها، أو إلحاق الضرر بها بأيّ شكل من الأشكال، ومع تطوّر وسائل التقنية الحديثة أصبحت المعلومات معرضة للخطر أكثر من السابق، وظهرت الحاجة الماسة إلى علم أمن المعلومات.



9- الهجمات الالكترونية و الحماية منها

أشهر الهجمات الالكترونية المعاصرة :

1 هجمات البرامج (أو الأكواد) الخبيثة (Malicious Code Attacks)

تشمل هجمات البرامج الخبيثة بشكل أساسي: هجمات فيروسات وديدان الحاسب الآلي، وبرامج أحصنة طروادة، وبرامج الاختراق، وبرامج التجسس الإلكتروني. وقد تتسبب هذه البرامج في أضرار كثيرة تتراوح ما بين مجرد الإزعاج، إلى فقد البيانات، ووصولاً إلى سرقة الأموال.

2 هجمات الأبواب الخلفية (Back Door Attacks)

في بعض الأحيان، يترك المصمّمون أو المبرمجون أو فنيو الصيانة طرقاً خفية، تسمّى الأبواب الخلفية، للوصول إلى الأجهزة والشبكات من أجل استخدامها لاحقاً لأعمال التطوير والصيانة عن بُعد، ويستغلّ المهاجمون هذه الطُّرق عند اكتشافها كأبواب خلفية للدخول إلى الأجهزة والشبكات بطرق غير شرعية.

9- الهجمات الالكترونية و الحماية منها

كسر كلمات المرور (Password Crack)

3

نعني بكسر كلمات المرور هنا عملية إعادة حساب كلمات المرور من البصمات الرقمية (Hash Values) لهذه الكلمات، التي تُحفظ عادة في ملفات خاصة بذلك، ويمكن تنفيذ هذا النوع من الهجوم إما بإعادة حساب البصمة الرقمية لكلمات المرور بطرق رياضية معقدة، أو من خلال الجمع بين هذه الطريقة وهجمات المعجم (Dictionary Attack). وما يتم عمله هو حساب البصمة الرقمية لكل كلمة تنتج من هجوم المعجم، ثم مقارنتها مع البصمة الرقمية المخزنة في النظام المراد الهجوم عليه، وفي حال مطابقة هذه القيم فهذا يعني أنه تم الحصول على كلمة المرور، وأما إذا اختلفت فيجري الانتقال لكلمة المرور التي تليها ... وهكذا. وهنا



9- الهجمات الالكترونية و الحماية منها

الهجوم الأعمى (الاستقصائي) (Brute Force Attack)

4

يسمى الهجوم الذي يحدث عن طريق تجريب جميع الاحتمالات الممكنة لكلمات المرور أو الأرقام السرية، أو أي معلومة يحتاج إليها المهاجم في عملية الهجوم بالهجوم الأعمى أو الاستقصائي. وسمي بهذا الاسم لأنه لا يعتمد على أي عملية حسابية، أو أي عملية لتسريع الهجوم أو اختصار الوقت للقيام بتنفيذه، وإنما يحصل بمحاولة الدخول مرة تلو الأخرى واستقصاء جميع الاحتمالات الممكنة. عادة ما يستخدم هذا النوع من الهجوم على الحسابات أو أسماء المستخدمين المشهورة التي تكون أثناء تنصيب الأنظمة، مثل حساب مدير النظام (Administrator) أو (Admin)، أو حساب الضيف (Guest). وهنا تبرز أهمية تغيير هذه الحسابات من الأسماء الافتراضية لها المحددة من الشركات المنتجة إلى أسماء أخرى خاصة بالمنشأة، وكذلك أهمية تغيير الإعدادات التلقائية التي يمكن النفاذ من خلالها، مثل إعدادات المشاركة في الملفات والطابعات.



9- الهجمات الالكترونية و الحماية منها



هجمات الرجل في الوسط (Man-in-the-Middle Attacks)

5

يُطلق على هذا الهجوم أيضًا هجوم اختطاف بروتوكول النقل (TCP Hijacking) (TCP Attack). ويحدث في هذا الهجوم التقاط حزم البيانات (Data Packets) المارة في الشبكة، ثم تغييرها، ثم إعادة إرسالها مرة أخرى إلى الشبكة لتكمل مسارها، لكن بمعلومات معدلة، فيمكن من خلال هذا الهجوم تعديل البيانات، أو الحذف منها، أو الزيادة عليها، أو تزويرها، أو تحويلها، أو إعادة توجيهها. ومن أشهر استخدامات هذا الهجوم انتحال هوية جهاز (أو مكوّن) آخر في الشبكة، خاصة عند الهجوم على عملية توزيع مفاتيح التشفير باستخدام الشهادات (Digital Certificates) فيظهر المهاجم كأنه رجل (غير مرئي) في الوسط بين الجهازين اللذين تجري عملية تبادل مفاتيح التشفير بينهما، فينتحل شخصية أحدهما، ثم يتعامل مع الآخر كأنه الجهاز (أو المكوّن) الحقيقي المقابل له، ومن ثم يمكن الحصول على معلومات مفاتيح التشفير، انظر الشكل .

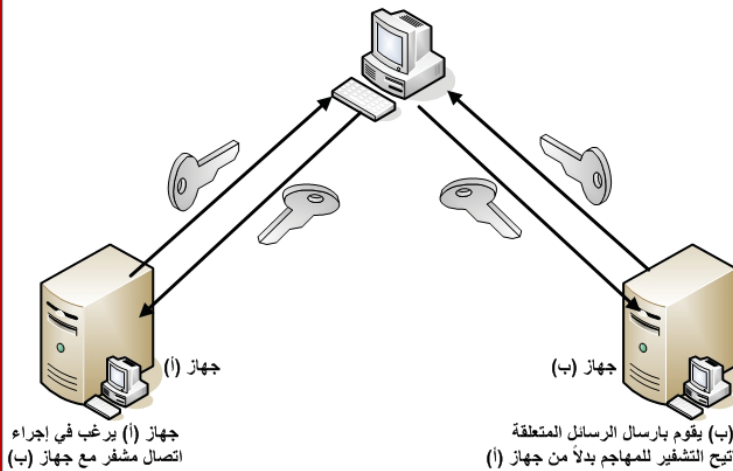
19

9- الهجمات الالكترونية و الحماية منها



5

المهاجم (الرجل في الوسط) يقوم باعتراض الاتصال بين جهاز (أ) وجهاز (ب)
ثم يقوم بالعمل وكأنه جهاز (ب) ويرسل مفتاح التشفير الخاص به إلى جهاز (أ)
ثم يقوم بإنشاء اتصال مشفر مع جهاز (ب) وكأنه جهاز (أ)



9- الهجمات الالكترونية و الحماية منها



هجوم تعطيل الخدمة (Denial of Service (DoS) Attack)

6

في هذا النوع من الهجوم يُرسل عدد هائل من طلبات الاتصال أو أوامر بروتوكولات الشبكات، مثل أمر (ping) إلى الجهاز الضحية من أجل إغراقه في معالجة هذا الطلبات، وتحمله أكثر من طاقته حتى وصوله لدرجة عدم الاستجابة، ومن ثم عدم قدرته على القيام بمهامه المعتادة، وقد تصل درجة الإغراق في بعض الأحيان إلى تعطيل الهدف نهائياً وخروجه من الخدمة. وهناك نوع خطير من هذه الهجمات يسمى هجوم تعطيل الخدمة الموزع (Distributed Denial of Service (DDoS) Attack)، والذي يتم فيه توزيع البرامج المصدرة لسلسلة من طلبات و أوامر الإغراق عبر عدد كبير من الأجهزة الموزعة في أماكن مختلفة التي تعمل عن بُعد، ومن ثم برمجة جميع هذه الأجهزة للهجوم معاً على الجهاز الضحية، ومن ثم إغراقه وتعطيله وإخراجه من الخدمة في وقت قصير. ويُعد هذا النوع من الهجمات من أعتى الهجمات وأكثرها ضراوة، حيث لا توجد له حلول مباشرة مخصصة له، وإنما تتم مكافحته بتكاتف عدد من الحلول.

9- الهجمات الالكترونية و الحماية منها



هجمات الخداع (Spoofing Attacks)

7

هي طريقة للتمكّن من الوصول إلى الأجهزة بطريقة غير شرعية عن طريق خداع هذه الأجهزة، بإرسال رسائل مخادعة تحتوي عنوان إنترنت (IP) يجعل الرسالة تبدو كأنها قادمة من جهة موثوقة. وإتمام هذا النوع من الهجوم فلا بدّ للمهاجم من استخدام طُرق وأدوات الحصول على عنوان الإنترنت (IP) المناسب الذي يستطيع من خلاله خداع الجهاز الضحية، وكذلك الحصول على برامج يستطيع من خلالها تغيير المعلومات الموجودة في جزء الرأس من حزم البيانات (Packet Header) لتظهر هذه الحزم كأنها قادمة من جهة موثوقة ومعروفة لدى الجهاز الضحية. وهنا تبرز الحاجة لأنظمة أمن المعلومات التي تستطيع كشف ذلك ومجابهته، خاصّة على مستوى الموجهات وجدران الحماية.





9- الهجمات الإلكترونية و الحماية منها

8

الرسائل غير المرغوب فيها (أو المزعجة) (Spam)

يُرَدُّ إلى صناديق البريد الإلكتروني كثير من الرسائل (المزعجة) غير المرغوب فيها. ويُعدُّ كثير من الناس أنَّ هذه الرسائل لا تُعدُّ هجمات إلكترونية، لكن واقع الحال يقول إن كثيراً منها يحتوي ملفات بها برامج أو أكواد خبيثة. ويمكن التخلص من هذا النوع من الرسائل بتفعيل عمليات التنقيح والفلتر الموضوعة في خوادم البريد الإلكتروني وكذلك بتوعية المستخدمين بحذف جميع الرسائل غير المرغوب فيها، وعدم الثقة في هذا النوع من الرسائل، وعدم فتحها.



9- الهجمات الإلكترونية و الحماية منها

9

هجمات التشمم أو الالتقاط (Sniffer Attacks)

المتشمم هو برنامج أو جهاز يراقب البيانات المارة عبر الشبكة ويلتقطها، ويمكن أن يكون هناك تشمم أو التقاط شرعي لمراقبة الشبكة ومتابعتها وإدارتها، ويمكن أن يكون غير شرعي لسرقة البيانات. ويُعدُّ هذا الهجوم خطيراً جداً على الشبكة لأنه يمكن زرع المتشمم في أي مكان في الشبكة، وغالباً لا يمكن كشفه، وهذا ما يجعله محبباً لدى المهاجمين. ويزداد الأمر خطورة إذا كان نقل المعلومات يجري على الشبكة، سواء أكانت محلية (LAN) أم واسعة (WAN)، في شكلها الأصلي غير مشفرة، لأنَّ المتشمم في هذه الحالة يستطيع قراءة كلمات المرور وكذلك محتويات الملفات النصية مثل ملفات معالجة الكلمات. وهنا تبرز أهمية توفير أنظمة الحماية التي تكشف وجود برامج وأجهزة التشمم وتكافحها، وكذلك الأنظمة التي تحول دون الاستفادة من المعلومات المسروقة في حالة نجاح المتشمم في سرقتها، كأن تكون مشفرة مثلاً.





9- الهجمات الالكترونية و الحماية منها

هجمات الهندسة الاجتماعية (Social Engineering Attacks)

10

يخلط هذا النوع من الهجوم بين النواحي الاجتماعية واهتمامات الناس وبين المهارات الفنية في خداع الضحايا وكسب ثقتهم للإدلاء بمعلومات سرية يتم استغلالها لسرقة المعلومات والأموال إلكترونياً (انظر الفصل السابع: موضوع: التهديدات الرقمية لشبكات الحاسب الآلي). وقد انتشر هذا النوع من الهجوم في الآونة الأخيرة انتشاراً كبيراً؛ لأنه لا يعتمد على كسر أنظمة الحماية التقنية التي تطورت مع مرور الوقت، وإنما يعتمد على كسب ثقة الضحايا وإيهامهم بأن من يطلب منهم معلوماتهم السرية (كاسم المستخدم وكلمة المرور وأرقام بطاقات الائتمان) هو جهة موثوقة (مصرف مثلاً) وبعد ذلك يتم استغلال هذه المعلومات وانتحال شخصيات الضحايا ومن ثم سرقتهم إلكترونياً عن طريق دخول يبدو شرعياً لأنظمة الحماية.



9- الهجمات الالكترونية و الحماية منها

هجوم تصفح الكتف (Shoulder Surfing Attack)

11

يعني هجوم تصفح الكتف أن يطلع المهاجم على المعلومات المهمة والحساسة كما لو كان ينظر إليها من فوق كتف الضحية، ويرى لوحة المفاتيح وما يقوم بضغطه من أزرار وما يعرض على الشاشة من معلومات. ويستخدم هذا الهجوم في الأماكن العامة أو أماكن العمل المشتركة، حيث ينظر المهاجم خلسة إلى شاشة الضحية، ومن ثم يعرف بعض المعلومات السرية، التي يجب أن لا يعرفها. ومن الأمثلة على ذلك: استراق النظر خلسة إلى الأرقام السرية لبطاقات الصرف الآلي وقت إدخال مستخدمها لها، وكذلك معرفة كلمات المرور للحسابات الآلية أو أجهزة الهاتف النقال وقت إدخالها، انظر الشكل .





9- الهجمات الالكترونية و الحماية منها

11

